

Personal data of 143 million US consumers compromised in massive Equifax server hack

Kevin Reed
11 September 2017

In possibly the largest and most damaging data breach ever, the credit reporting company Equifax announced on September 7 that the personal information of 143 million US consumers—including their names, Social Security numbers, addresses and birth dates—had been hacked and stolen from its servers between mid-May and July of this year.

According to a company press release, Equifax executives discovered on July 29 that cybercriminals “exploited a U.S. website application vulnerability to gain access to certain files.” However, the company did nothing to immediately notify the public. Instead, Equifax “engaged a leading, independent cybersecurity firm that has been conducting a comprehensive forensic review” for six weeks before reporting the data theft.

In other words, the \$18 billion corporation with principal responsibility for storing and protecting the most sensitive personal information of more than half of all US adults had its servers hacked, covered up the breach for two-and-a-half months, and still claims to not know what happened.

In a hastily prepared video statement posted Thursday on YouTube, Equifax CEO Richard F. Smith made the remarkable claim that his firm is “focused on consumer protection” and has “developed a comprehensive portfolio of services to support all U.S. consumers,” including one year of free credit reporting and identity fraud protection, a service that normally costs \$19.95 per month.

However, Smith’s offer has since been exposed as a ruse to get individuals who sign up to accept terms of service that effectively relinquishes their right to seek any future legal action against the corporation. A class-action lawsuit worth as much as \$70 billion was announced in Oregon, and the value of Equifax stock fell by nearly 14 percent on Wall Street on Friday.

The extraordinary security incompetence and legal swindling at Equifax has now been combined with a report that a few days after the July 29 discovery of the breach, three company executives sold off \$1.8 million of their company shares.

Bloomberg reported on Thursday that Equifax CFO John Gamble; President of US Information Solutions Joseph Loughran; and President of Workforce Solutions Rodolfo Ploder sold stock worth \$946,374, \$584,099 and \$250,458 (13 percent, 9 percent and 4 percent of their holdings), respectively, by August 2. The company has since made the claim that the executives had not been informed of the hack.

Equifax is one of three major US consumer credit reporting agencies (the other two are TransUnion and Experian) that track, evaluate and rate the borrowing and repayment history of individuals in the US and internationally. Financial institutions such as banks, mortgage companies, auto and other consumer lending organizations use the information provided by these agencies—summarized as a FICO (Fair Isaac Corporation) score of between 350 and 800 points—to make decisions about credit limits, interest, and insurance rates.

The Equifax data theft follows a series of hacking episodes that have impacted sensitive consumer information: 500 million Yahoo accounts, 145 million eBay accounts, and 76 million Chase accounts are among the most notable.

In addition to the primary personal information, Equifax reported that the data breach compromised 209,000 credit card numbers and the drivers’ license numbers of possibly as many as 182,000 consumers. Other stolen information could also include credit account security questions and answers.

This is not the first security failure at Equifax.

According to security expert Brian Krebs, hackers were able to access tax data of employees at companies using Equifax’s payroll service subsidiary TALX last May. According to Krebs, the credit bureaus have “shown themselves to be terrible stewards of very sensitive data” due to a lack of government oversight and regulation.

As an arm of the investment services industry, the consumer credit reporting agencies exist to serve the interests of the giant banks and the financial oligarchy and view the public as a target of exploitation and source of profit. Equifax, TransUnion, and Experian have been used increasingly since the Great Recession of 2008 as an instrument for intensifying economic inequality and squeezing ever more wealth out of the pockets of the working class and into the coffers of the super-rich.

Identity theft is a serious threat for millions whose information is now circulating and can be used to fraudulently validate their identity and open bank accounts or take out loans in their name. This information can also be used by hackers to change passwords and other settings on existing bank and credit accounts.

The consequences for working people of having their credit data compromised are devastating. For example, with millions of people relying upon credit to make ends meet—average household balance-carrying credit card debt in the US is \$16,000—a fraudulent transaction or change in a credit score can lead to a dramatic reduction in living standards or a forced personal bankruptcy.



To contact the WSWWS and the
Socialist Equality Party visit:

wsws.org/contact